AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

District of Oregon

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Premises at 4303 SE 76th Avenue, Portland, Oregon and Person of Juan Carlos Ramon, each further described in Attachment A

Case No. '17-MC-592 A-B

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

4303 SE 76th Avenue, Portland, OR and Juan Carlos Ramon, further described in Attachment A, incorporated herein

located in the _____ District of Oregon, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, incorporated by reference herein.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. 2251(a) and (e); and 2252A(a)(1), (a)(2)(A),(a)(5)(B), (a)(6) and (b)(1) and (2)	production/attempted production of child pornography; transportation, receipt, distribution, possession, and access with intent to view child pornography, and attempts of same; sending depiction to induce minor to participate in illegal activity

The application is based on these facts:

See Attached Affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Sworn via telephone on 11/15/17 at 4:13 pm pursuant to FRCP 4.1. -YYY

Applicant's signature

James W. Humphrey, Jr., FBI Task Force Officer

Printed name and title

Sworn to before me and signed via telephone. ~~in my presence.~~

Date: 11/15/2017

Judge's signature

City and state: Portland, Oregon

YOULEE Y. YOU, United States Magistrate Judge

Printed name and title

Print Save As... Attach Reset

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANTS

INTRODUCTION

I, James W. Humphrey, Jr., having been first duly sworn, do hereby depose and state as follows:

1. I have been employed as a Deputy Sheriff for the Ouachita Parish Sheriff's Office in Monroe, Louisiana since August 2001. I am currently assigned to the Federal Bureau of Investigation, New Orleans, Louisiana Division, Monroe Resident Agency as a Task Force Officer, and have been since November 2013. I am also currently assigned to the Internet Crimes Against Children (ICAC) Task Force, and have been since November 2013. While assigned to the FBI and ICAC Task Force, I have investigated federal and state criminal violations, and assisted in federal and state investigations, related to high technology or cyber crime, child exploitation, and child pornography violations. I have gained experience through training provided by the Federal Bureau of Investigation and the Louisiana Attorney General's Office Internet Crimes Against Children Unit, along with everyday work relating to conducting these types of investigations. In my work with the FBI and the ICAC Task Force, I have observed and reviewed numerous examples of child pornography as defined in 18 U.S.C. § 2256, in all forms of media including computer media. Moreover, I am a Special Federal Officer/Special Deputy United States Marshal engaged in enforcing federal criminal laws, including 18 U.S.C. §§ 2251 and 2252A, and am authorized by the Attorney General to request a search warrant.

2. I submit this application and affidavit in support of search warrants authorizing a search of the premises located at 4303 SE 76th Avenue, Portland, Oregon, further described in Attachment A, incorporated herein by reference (hereinafter the "SUBJECT PREMISES"), as

well as the person of JUAN CARLOS RAMON, DOB 2/10/85, further described in Attachment A, and to seize all evidence, fruits, and instrumentalities of the child pornography offenses discussed below, further described in Attachment B, incorporated herein by reference, that are located on the SUBJECT PREMISES and on JUAN CARLOS RAMON. As set forth below, I have probable cause to believe that contraband, evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2251(a) and (e) (Production and Attempted Production of Child Pornography), 2252A(a)(1) and (b)(1) (Transportation and Attempted Transportation of Child Pornography); 2252A(a)(2)(A) and (b)(1) (Receipt, Distribution, and Attempted Receipt and Distribution of Child Pornography); 2252A(a)(5)(B) and (b)(2) (Possession of, and Knowingly Accessing or Attempting to Access With Intent to View Child Pornography), and 2252A(a)(6) (Sending a Minor a Visual Depiction That Is or Appears to Be of a Minor Engaging in Sexually Explicit Conduct, for the Purpose of Inducing a Minor to Participate in Unlawful Activity) are located on the SUBJECT PREMISES and on the person of JUAN CARLOS RAMON. I request authority to search the entire SUBJECT PREMISES, including the residential dwelling, carport, and any outbuildings, and any computer and computer media located therein and on the person of JUAN CARLOS RAMON, where the items specified in Attachment B may be found, and to seize all items listed in Attachment B as contraband and instrumentalities, fruits, and evidence of the crimes described herein.

3. The statements contained in this affidavit are based in part on: information provided by FBI Special Agents; written reports about this and other investigations that I have received, directly or indirectly, from other law enforcement agents; information gathered from the service of administrative subpoenas; the results of physical surveillance conducted by law enforcement agents; independent investigation and analysis by FBI agents, analysts, and computer forensic

professionals; and my experience, training and background as a Task Force Officer with the FBI and the ICAC Task Force. Because this affidavit is being submitted for the limited purpose of securing authorization for the requested search warrants, I have not included each and every fact known to me concerning this investigation. Instead, I have set forth only the facts that I believe are necessary to establish probable cause for the requested warrants.

RELEVANT STATUTES

4. This investigation concerns alleged violations of: 18 U.S.C. §§ 2251(a) and (e), Production and Attempted Production of Child Pornography; 2252A(a)(1) and (b)(1), Transportation and Attempted Transportation of Child Pornography; 2252A(a)(2)(A) and (b)(1), Receipt, Distribution, and Attempted Receipt and Distribution of Child Pornography; 2252A(a)(5)(B) and (b)(2), Possession of, and Accessing or Attempting to Access with Intent to View, Child Pornography; and 2252A(a)(6), Sending a Minor a Visual Depiction of a Minor Engaging in Sexually Explicit Conduct for the Purpose of Inducing a Minor to Participate in Unlawful Conduct.

a. 18 U.S.C. §§ 2251(a) and (e) prohibit a person from using, persuading, inducing, or enticing a minor to engage in any sexually explicit conduct, or attempts to do so, for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting a live visual depiction of such conduct, if: such person knows or has reason to know that such visual depiction will be transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce; the visual depiction was produced or transmitted using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer; or such visual depiction has actually been

transported or transmitted using any means or facility in interstate or foreign commerce or in or affecting interstate or foreign commerce;

b. 18 U.S.C. §§ 2252A(a)(1) and (b)(1) prohibit a person from knowingly transporting or attempting to transport, using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce by any means, including by computer, any child pornography;

c. 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1) prohibit a person from knowingly receiving, distributing, or attempting to receive or distribute any child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer;

d. 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2) prohibit a person from knowingly possessing, or knowingly accessing or attempting to access with intent to view, any material that contains an image of child pornography that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer; and

e. 18 U.S.C. §§ 2252A(a)(6) prohibits a person from knowingly distributing, sending, or providing to a minor any visual depiction that is, or appears to be, of a minor engaging in sexually explicit conduct, which distribution, sending, or provision is accomplished using any means or facility of interstate or foreign commerce, for the purpose of inducing or persuading a minor to participate in any activity that is illegal.

DEFINITIONS

5. The following definitions apply to this Affidavit and attachments hereto:

a. "Bulletin Board" means an Internet-based website that is either secured (accessible with a password) or unsecured, and provides members with the ability to view postings by other members and make postings themselves. Postings can contain text messages, still images, video images, or web addresses that direct other members to specific content the poster wishes. Bulletin boards are also referred to as "internet forums" or "message boards." A "post" or "posting" is a single message posted by a user. Users of a bulletin board may post messages in reply to a post. A message "thread," often labeled a "topic," refers to a linked series of posts and reply messages. Message threads or topics often contain a title, which is generally selected by the user who posted the first message of the thread. Bulletin boards often also provide the ability for members to communicate on a one-to-one basis through "private messages." Private messages are similar to e-mail messages that are sent between two members of a bulletin board. They are accessible only by the user who sent/received such a message, or by the Website Administrator.

b. "Chat" refers to any kind of communication over the Internet that offers a real-time transmission of text messages from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

c. "Child Erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, legally

obscene or that do not necessarily depict minors in sexually explicit conduct.

d. "Child Pornography," as used herein, is defined in 18 U.S.C. § 2256(8) as any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

e. "Computer," as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1) as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

f. "Computer Server" or "Server," as used herein, is a computer that is attached to a dedicated network and serves many users. A web server, for example, is a computer which hosts the data associated with a website. That web server receives requests from a user and delivers information from the server to the user's computer via the Internet. A domain name system ("DNS") server, in essence, is a computer on the Internet that routes communications when a user types a domain name, such as www.cnn.com, into his or her web browser. Essentially, the domain name must be translated into an Internet Protocol ("IP") address so the computer hosting the web site may be located, and the DNS server provides this function.

g. "Computer hardware," as used herein, consists of all equipment which can receive,

capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

h. "Computer software," as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

i. "Computer-related documentation," as used herein, consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.

j. "Computer passwords, pass-phrases and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password or pass-phrase (a string of alpha-numeric characters) usually operates as a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that

creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

k. "File Transfer Protocol" ("FTP"), as used herein, is a standard network protocol used to transfer computer files from one host to another over a computer network, such as the Internet. FTP is built on client-server architecture and uses separate control and data connections between the client and the server.

l. "Host Name." A Host Name is a name assigned to a device connected to a computer network that is used to identify the device in various forms of electronic communication, such as communications over the Internet.

m. "Hyperlink" refers to an item on a web page which, when selected, transfers the user directly to another location in a hypertext document or to some other web page.

n. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

o. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone based dial-up, broadband based access via digital

subscriber line ("DSL") or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name – a user name or screen name, an "e-mail address," an e-mail mailbox, and a personal password selected by the subscriber. By using a computer equipped with a modem, the subscriber can establish communication with an Internet Service Provider ("ISP") over a telephone line, through a cable system or via satellite, and can access the Internet by using his or her account name and personal password.

p. "Internet Protocol address" or "IP address" refers to a unique number used by a computer to access the Internet. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet. IP addresses are also used by computer servers, including web servers, to communicate with other computers.

q. Media Access Control ("MAC") address. The equipment that connects a computer to a network is commonly referred to as a network adapter. Most network adapters have a MAC address assigned by the manufacturer of the adapter that is designed to be a unique identifying number. A unique MAC address allows for proper routing of communications on a network. Because the MAC address does not change and is intended to be unique, a MAC address can allow law enforcement to identify whether communications sent or received at different times are associated with the same adapter.

r. "Minor" means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).

s. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks ("DVDs"), Personal Digital Assistants ("PDAs"), Multi Media Cards ("MMCs"), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

t. "Secure Shell" ("SSH"), as used herein, is a security protocol for logging into a remote server. SSH provides an encrypted session for transferring files and executing server programs.

u. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. See 18 U.S.C. § 2256(2).

v. "URL" is an abbreviation for Uniform Resource Locator and is another name for a web address. URLs are made of letters, numbers, and other symbols in a standard form.

People use them on computers by clicking a pre-prepared link or typing or copying and pasting one into a web browser to make the computer fetch and show some specific resource (usually a web page) from another computer (web server) on the Internet.

w. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

x. "Website" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language ("HTML") and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol ("HTTP").

THE MUSICAL.LY SOCIAL NETWORK SITE

6. According to public source information and my investigation to date, I know that musical.ly is a social network site on the Internet. The developer of musical.ly is a company called Musical.ly, Inc. ("Musical.ly"), which has headquarters in Shanghai, China, and offices in San Francisco, California.

7. Users can access musical.ly by downloading onto their computer (including a tablet or cellular phone) a free software application (commonly known as an "app"). Each user is required to provide a self-selected username and a means of identification, which can be a cellular telephone number.

8. A musical.ly user has the ability to generate a video, generally lasting between 15 seconds and 1 minute, which the user can then share with others using the site. Users generating videos may select sound tracks to accompany the videos, use different speed options (time-lapse, slow, normal, fast, and epic) and add pre-set filters and effects. Users of the site can browse

content uploaded by other users of the site, regardless of whether they create their own videos.

9. Users of musical.ly have the ability to "follow" certain users of interest and will receive notice when a followed user is online at the same time. Users of the site also have the ability to communicate privately with each other through a written chat format. Users can also download another free app (called live.ly) that allows them to create a live video stream (*e.g.*, of themselves engaged in activity). The user presenting on live.ly can make their presentation generally available or restrict it to a limited number of people, including a single user. Users watching the presentation can, through a written chat format, communicate with the user who is streaming the live video presentation; in particular, any chat messages will appear on the screens of all users watching the user who is doing the live presentation. Written chats between users are recorded by musical.ly and retained by the site for a period of time.

BACKGROUND OF THE INVESTIGATION AND PROBABLE CAUSE

10. On June 30, 2017, the Ouachita Parish (Louisiana) Sheriff's Office responded to a residence in Monroe, Louisiana in reference to an investigation. The initial responding patrol deputy made contact with the complainant. The deputy learned that complainant's six year old daughter and eight year old niece had been victimized on the internet. According to the complainant, the crimes occurred on or about June 28, 2017 when both juvenile victims were on the internet application (APP) known as Musical.ly. The victims were communicating with an individual that they thought was a young white female using the screen name of @lexithetiger (hereafter "the suspect"). During communication with the unknown suspect, both juvenile victims were manipulated into sending nude images and videos of themselves.

11. On July 8, 2017, I obtained a state search warrant for Musical.ly in response to the information received above. The search warrant was presented to and signed by a Fourth

Judicial District Court Judge for Ouachita and Morehouse Parishes in Louisiana. Musical.ly complied with the search warrant and provided all requested information. The following is a brief description of what the records revealed with regards to the two juvenile victims referenced in paragraph 10 above:

a) The suspect started the conversation by thanking the victims for following "her."

b) The suspect claimed to be bored and wanting to play a game. The victims agreed to participate in the game.

c) The suspect then told the victims that the suspect would send a picture of "herself" and in return, the victims would have to send a picture of themselves doing the same thing.

d) An image of a young (juvenile) white female's face was sent to the victims from the suspect's account and in return the victims sent a face image.

e) The suspect then exchanged a clothed body image with the victims.

f) The suspect then sent an image showing what appears to be the same young white female in her underwear and the victims sent an image of a similar pose.

g) The suspect then asked the victims if they wanted to keep going and told them that the poses were going to get harder to do. The victims agreed to continue to participate.

h) The exchange of pictures continued with the suspect exchanging images of exposed buttocks, frontal nudity, and exposed vaginal images. Each time, the victims responded with similar pictures in return to the suspect.

i) The suspect then sent a video of an unknown individual masturbating with a yellow writing marker. In response to the video, one of the victims told the suspect that they couldn't do that and the suspect responded that "she can rub it" and stated, "For 30 seconds." When the victims told the suspect that they didn't have anything to use, the

suspect replied, "Her fingers," "She can use her fingers." The suspect stated, "U can record the video and she can do that."

j) The victims then sent an image of them digitally masturbating.

k) The suspect continued to demand more images of the victims. The suspect sent the minors a video of two females performing oral sex on each other and claimed that it was "she" and her cousin. The suspect demanded five pictures from each of the minors and instructed the victims to get into certain positions, including "Have her take a pic of u with nothing on and ur legs apart all the way" and "But I wanna see her tongue on ur parts and ur tongue on her parts."

l) The victims then sent the suspect an image of them performing oral sex on each other.

12. There were many more images exchanged between the victims and the suspect. These interactions concluded with the eight-year-old victim sending the suspect a video of herself masturbating. In reviewing the records from Musical.ly, it appears there is a time zone and/or UTC time difference, as the records reflect the initial communication with the victims above occurred at approximately 2:01 in the morning on June 29, 2017, but the complainant stated it occurred on June 28, 2017 around 1:00 in the afternoon, and that it was not possible the communication occurred at 2:00 am on June 29. In addition, the records provided by Musical.ly revealed a second session with the eight-year-old victim after a gap in time, where the suspect asked the eight-year-old if her cousin was there and the victim replied "no." The records provided by Musical.ly reflect that this later communication occurred on June 30, 2017 at approximately eight minutes after midnight.

13. Investigators reviewed all of the other information, chat, image, and video logs provided by Musical.ly in reference to the @lexithetiger user account and determined that there were

many other juvenile victims that had sent nude images and videos to the suspect. The suspect followed a very similar pattern in his/her interaction with the other victims, asking if they wanted to play a game and then manipulating them into sending nude images and videos of themselves. In at least a couple screenshots of communications from the suspect to the victims, an image was circled and "Verizon" appeared at the top of the screen, indicating, from my training and experience, that at least those communications were sent using a smart phone.

14. In addition to the chat records and image/video exchanges, Musical.ly also provided investigators with Internet Protocol Addresses (IP Addresses) that the suspect was using during the criminal activities, and subscriber information. The subscriber information did not include a name or contact information other than an email address of lexithetiger@hotmail.co (not .com). The records reflect that the @lexithetiger account was created on June 24, 2017 with an "iPhone 8,2" while using IP Address 209.160.127.158. Investigators noted that during the criminal activity, the IP Addresses that were being used by the suspect would change multiple times. By researching the American Registry for Internet Numbers (ARIN), investigators learned that these IP Addresses were assigned to Paradise Networks LLC. Through research into Paradise Networks LLC., investigators learned that Paradise Networks LLC is, simply put, a server located in the United States that allows Switzerland based Golden Frog GmbH to conduct business domestically.

15. Golden Frog GmbH is a company that provides a paid service to anonymize their customers' identity while on the internet. With the assistance of the United States Department of Justice, Criminal Division, Office of International Affairs, an International Mutual Assistance Request in Criminal Matters was completed and served upon Golden Frog GmbH. Golden Frog GmbH complied with the request and supplied investigators with all requested information.

Golden Frog GmbH identified the customer as follows:

- JUAN CARLOS RAMON
- Customer ID number - 607416
- Customer Email Address - **carloshasmail@gmail.com**
- Credit Card Number - 481583XXXXXX0193 (VISA)
- Credit Card Zip Code 97206.

16. In addition, Golden Frog GmbH advised the services associated with the referenced IP Addresses started on June 3, 2017 @ 22:23:45 UTC using IP Address 76.115.129.102. Golden Frog GmbH also provided a list of IP Addresses that was captured while suspect was using the service. The list consists of the date, time, client IP Address and assigned IP Address. By comparing the date and time that the victims were victimized and the client IP Address that was signed into the Golden Frog GmbH service, investigators noted that IP Address 76.115.129.102 was the IP Address that was being used by the suspect. Investigators researched the IP Address using ARIN and learned that Comcast Cable Communications is the Internet Service Provider (ISP) that maintains and services this IP Address.

17. Investigators served Comcast Cable Communication with an administrative subpoena to obtain subscriber information. Comcast Cable Communications complied with the subpoena and investigators learned that the customer who was assigned IP Address 76.115.129.102 on the dates and times that the criminal activity took place is CARLOS RAMON at 4303 SE 76th Avenue, Portland, OR 972063353. The telephone number that is associated with the account is 626-616-2706 and the associated e-mail address is carloshasmail@comcast.net.

THE RESIDENCE

18. On October 19, 2017, an FBI Agent observed one vehicle parked in a carport to the side

of the residence located at 4303 SE 76th Avenue, Portland, Oregon 97206 (the SUBJECT PREMISES). This vehicle was a dark colored Honda Fit with Oregon License Plate 758 KBX. According to records of the Oregon Department of Motor Vehicles, this vehicle has been registered to JUAN RAMON and Hailey Foster since July 18, 2017. On November 14, 2017, the same FBI Agent drove by the SUBJECT PREMISES and saw the same Honda Fit parked in the carport to the side of the residence.

19. The residence located at 4303 SE 76th Avenue, Portland, Oregon 97206 is described as a detached, blue, single family home with white shutters and a front porch. The house number, 4303, is displayed on the front of the home. A photograph of the SUBJECT PREMISES is contained in Attachment A.

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

20. Computers and digital technology have dramatically changed the way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

21. Child pornographers can now transfer printed photographs into a computer-readable format with a device known as a scanner. Furthermore, with the advent of digital cameras, when the photograph is taken it is saved as a digital file that can be directly transferred to a computer by simply connecting the camera to the computer. In the last ten years, the resolution of pictures taken by digital cameras has increased dramatically, meaning the photos taken with digital cameras have become sharper and crisper. Photos taken on a digital camera are stored on a removable memory card in the camera. These memory cards often store up to 32 gigabytes of data, which provides enough space to store thousands of high-resolution photographs. Video camcorders, which once recorded video onto tapes or mini-CDs, now can save video footage in a digital format

directly to a hard drive in the camera. The video files can be easily transferred from the camcorder to a computer.

22. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (FTPs) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "Instant Messaging"), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials.

23. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. In addition, there are numerous options available for the storage of computer or digital files. One-Terabyte external and internal hard drives are not uncommon. Other media storage devices include CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices which are plugged into a port on the computer. It is extremely easy for an individual to take a photo with a digital camera, upload that photo to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices (CDs and DVDs are unique in that special software must be used to save or "burn" files onto them). Media storage devices can easily be concealed and carried on an

individual's person.

24. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

25. Individuals also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer or external media in most cases.

26. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

27. I know based on my training and experience, and based on conversations I have had with others who investigate child exploitation offenses, including child pornography offenses, that people who have a sexual interest in children, including persons who collect and trade child pornography, often receive sexual gratification from images and video clips depicting the sexual

exploitation of children. They may also use such images and videos to lower the inhibitions of children who they wish to sexually abuse or exploit. Such persons often maintain their collections of child pornography in safe, secure, and private locations, such as their residence, and on computers and digital storage media under their direct control, including on smart phones or thumb drives that they carry on their person. Such persons often maintain their collections, which are considered prized possessions, for long periods of time, and prefer not to be without their collections for any prolonged period of time. In some recent cases, however, some persons with a sexual interest in children have been found to download and delete child pornography on a cyclical and repetitive basis, rather than storing a collection of child pornography indefinitely.

SEIZURE AND SEARCH OF DIGITAL DEVICES

28. As described above and in Attachment B, this application seeks permission to search for records that might be found on the SUBJECT PREMISES and on the person of JUAN CARLOS RAMON, in whatever form they are found. One form in which the records will likely be found is data stored on a computer's hard drive, on other storage media, or other digital devices, including cell phones (hereinafter collectively referred to as digital devices). Thus, the warrant applied for would authorize the seizure of electronic storage media or the copying of electronically stored information, all under Rule 41(e)(2)(B).

29. There is probable cause to believe, and I do believe, that relevant records will be stored on one or more digital devices based on the facts above and because, based on my knowledge, training, and experience, I know:

a. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a digital device, deleted, or viewed via the Internet. Electronic files downloaded to a digital device can be stored for years at little or no cost. Even

when files have been deleted, they can be recovered months or years later using forensic tools. When a person "deletes" a file on a digital device, the data contained in the file does not actually disappear; rather, that data remains on the digital device until it is overwritten by new data. Therefore, deleted files or remnants of deleted files, may reside in free space or slack space—that is, in space on the digital device that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a digital device's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

b. Wholly apart from user-generated files, digital devices—in particular, internal hard drives—contain electronic evidence of how a digital device has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Digital device users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

c. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

d. Based on actual inspection of other evidence related to this investigation, discussed above, I am aware that one or more digital devices were used to commit the offenses described herein from the SUBJECT PREMISES, and that the suspect used a smart phone on at least a couple occasions to commit the offenses. Thus, there is reason to believe that there is a digital device currently located on the SUBJECT PREMISES. In addition, given the above and the frequency with which persons carry smart phones on their person, there is also reason to believe that a digital device will be located on JUAN CARLOS RAMON.

30. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant but also for forensic electronic evidence that establishes how digital devices were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any digital device at the SUBJECT PREMISES and on the person of JUAN CARLOS RAMON, because, based on my knowledge, training, and experience, I know:

a. Data on the digital device can provide evidence of a file that was once on the digital device but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the digital device that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the digital device was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a digital device can also indicate who has used or controlled it. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, email, email address books, "chat," instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or

controlled the digital device at a relevant time. Further, forensic evidence on a digital device can show how and when it was accessed or used. Such "timeline" information allows the forensic analyst and investigators to understand the chronological context of access to the digital device, its use, and events relating to the offense under investigation. This "timeline" information may tend to either inculpate or exculpate the user of the digital device. Last, forensic evidence on a digital device may provide relevant insight into the user's state of mind as it relates to the offense under investigation. For example, information on a digital device may indicate the user's motive and intent to commit a crime (e.g., relevant web searches occurring before a crime indicating a plan to commit the same), consciousness of guilt (e.g., running a "wiping program" to destroy evidence on the digital device or password protecting or encrypting such evidence in an effort to conceal it from law enforcement), or knowledge that certain information is stored on a digital device (e.g., logs indicating that the incriminating information was accessed with a particular program).

c. A person with appropriate familiarity with how a digital device works can, after examining this forensic evidence in its proper context, draw conclusions about how digital devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a digital device that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a digital device is evidence may depend on other information stored on the digital device and the application of knowledge about how a

digital device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a digital device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a digital device. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's knowledge or intent.

f. I know that when an individual uses a digital device to commit the crimes described in this affidavit, the individual's digital device will generally serve both as an instrumentality for committing the crime and also as a storage medium for evidence of the crime. The digital device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The digital device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a digital device used to commit a crime of this type may contain: data that is evidence of how the digital device was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

31. In most cases, a thorough search of the Premises for information that might be stored on a digital device requires the seizure of the device and a later, off-site review consistent with the warrant. In lieu of removing a digital device from the Premises, it is sometimes possible to image or copy it. Generally speaking, imaging is the taking of a complete electronic picture of the digital device's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the digital device

and to prevent the loss of the data either from accidental or intentional destruction. This is true because:

a. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a digital device has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine digital devices to obtain evidence. Digital devices can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Records sought under this warrant could be stored in a variety of formats that may require off-site reviewing with specialized forensic tools. Similarly, digital devices can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the digital device off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

32. Because it appears that at least two people share the SUBJECT PREMISES as a residence, it is possible that the SUBJECT PREMISES will contain digital devices that are predominantly used, and perhaps owned, by one or more persons who are not suspected of a

crime. If it is nonetheless determined that it is possible that the things described in this warrant could be found on any of those digital devices, the warrants applied for would permit the seizure and review of those items as well.

33. Based on the facts above, and based on my training and experience, it is likely that the SUBJECT PREMISES and/or JUAN CARLOS RAMON will contain/have at least one Apple brand device, such as an iPhone or iPad, because the subscriber records from Musical.ly indicated that the suspect used an "iphone 8,2" to set up the @lexithetiger account.

34. I know from my training and experience, as well as from information found in publicly available materials including those published by Apple, that some models of Apple devices such as iPhones and iPads offer their users the ability to unlock the device via the use of a fingerprint or thumbprint (collectively, "fingerprint") in lieu of a numeric or alphanumeric passcode or password. This feature is called Touch ID.

35. If a user enables Touch ID on a given Apple device, he or she can register up to 5 fingerprints that can be used to unlock that device. The user can then use any of the registered fingerprints to unlock the device by pressing the relevant finger(s) to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) found at the bottom center of the front of the device. In my training and experience, users of Apple devices that offer Touch ID often enable it because it is considered to be a more convenient way to unlock the device than by entering a numeric or alphanumeric passcode or password, as well as a more secure way to protect the device's contents. This is particularly true when the user(s) of the device are engaged in criminal activities and thus have a heightened concern about securing the contents of the device.

36. In some circumstances, a fingerprint cannot be used to unlock a device that has Touch ID enabled, and a passcode or password must be used instead. These circumstances include: (1) when more than 48 hours has passed since the last time the device was unlocked; and (2) when the device has not been unlocked via Touch ID in 8 hours and the passcode or password has not been entered in the last 6 days. Thus, in the event law enforcement encounters a locked Apple device, the opportunity to unlock the device via Touch ID exists only for a short time. Touch ID also will not work to unlock the device if (1) the device has been turned off or restarted; (2) the device has received a remote lock command; and (3) five unsuccessful attempts to unlock the device via Touch ID are made.

37. The passcode or password that would unlock the Apple device found during the search of the SUBJECT PREMISES and JUAN CARLOS RAMON is not known to law enforcement. Thus, it will likely be necessary to press the fingers of the users of the Apple device found during the search of the SUBJECT PREMISES and JUAN CARLOS RAMON to the device's Touch ID sensor in an attempt to unlock the device for the purpose of executing the search authorized by the requested warrants. Attempting to unlock the relevant Apple device(s) via Touch ID with the use of the fingerprints of the users is necessary because the government may not otherwise be able to access the data contained on those devices for the purpose of executing the search authorized by these warrants.

38. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose fingerprints are among those that will unlock the device via Touch ID, and it is also possible that the person in whose possession the device is found is not actually a user of that

device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require any occupant of the SUBJECT PREMISES to press their fingers against the Touch ID sensor of the locked Apple device found during the search of the SUBJECT PREMISES and JUAN CARLOS RAMON in order to attempt to identify the device's user(s) and unlock the device(s) via Touch ID. Based on these facts and my training and experience, it is likely that JUAN CARLOS RAMON (a/k/a CARLOS RAMON and JUAN RAMON) is one user of the device(s) and thus that his fingerprints are among those that are able to unlock the device via Touch ID.

39. Although I do not know which of a given user's 10 fingerprints is capable of unlocking a particular device, based on my training and experience I know that it is common for a user to unlock a Touch ID-enabled Apple device via the fingerprints on thumbs or index fingers. In the event that law enforcement is unable to unlock the device(s) found in the SUBJECT PREMISES or on JUAN CARLOS RAMON as described above within the five attempts permitted by Touch ID, this will simply result in the device requiring the entry of a password or passcode before it can be unlocked.

40. I therefore request that the Court authorize law enforcement to press the fingers, including thumbs, of the above-named individuals found at the SUBJECT PREMISES to the Touch ID sensor of the device(s), such as an iPhone or an iPad, found at the SUBJECT PREMISES or on JUAN CARLOS RAMON for the purpose of attempting to unlock the device(s) via Touch ID in order to search the contents as authorized by the requested warrants.

41. *Nature of the examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrants for which I apply would permit seizing, imaging, or otherwise copying digital devices that reasonably appear to contain some or all of the evidence described in the warrants and would authorize a later review of the device or information consistent with the warrants. The later review may require techniques, including but not limited to computer-assisted scans of the entire device, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrants.

42. The initial examination of the digital device will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrants. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrants. The government shall complete this review within 180 days of the date of execution of the warrants. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

43. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the digital device do not contain any data falling within the scope of the warrants, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrants, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrants, through the conclusion of the case.

44. If an examination is conducted, and the digital device does not contain any data falling within the ambit of the warrant, the government will return the digital device to its owner within

a reasonable period of time following the search and will seal any image of the digital device, absent further authorization from the Court.

45. The government may retain the digital device as evidence, fruits, contraband, or an instrumentality of a crime or to commence forfeiture proceedings against the digital device and/or the data contained therein.

46. The government will retain a forensic image of the digital device for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

47. The government has not made any prior efforts in other judicial fora to obtain evidence sought under the warrants, except as stated above.

MISCELLANEOUS

48. As mentioned above, records received from Golden Frog GmbH revealed that JUAN CARLOS RAMON paid for that service to anonymize his identity while on the internet in June 2017, using a VISA credit card, number 481583XXXXXX0193. I know from my training and experience that individuals typically keep their credit cards in a wallet on their person, or in their home. Thus, there is probable cause to believe that this credit card will be found at the SUBJECT PREMISES or on the person of JUAN CARLOS RAMON, and seizure of the card will be relevant evidence of JUAN CARLOS RAMON's identity as the actual user of the @lexithetiger account to perpetrate the offenses discussed above.

///

CONCLUSION

49. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that contraband and evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B, are located at the SUBJECT PREMISES, described in Attachment A, and on the person of JUAN CARLOS RAMON. I therefore respectfully request that this Court issue search warrants for the SUBJECT PREMISES and for the person of JUAN CARLOS RAMON, authorizing the seizure and search of the items described in Attachment B.

50. This affidavit, the accompanying application, and the requested search warrants were reviewed by Assistant United States Attorney Jane Shoemaker prior to being submitted to the Court. AUSA Shoemaker informed me that in her opinion the affidavit and application are legally and factually sufficient to establish probable cause to support the issuance of the requested warrants.

Sworn via telephone on 11/15/17 at 4:13 pm pursuant to FRCP 4.1. -YYY

JAMES W. HUMPHREY, JR.
Task Force Officer,
Federal Bureau of Investigation

via telephone
Subscribed and sworn to ~~before me~~ this 15th day of November 2017.

HONORABLE YOULEE Y. YOU
United States Magistrate Judge

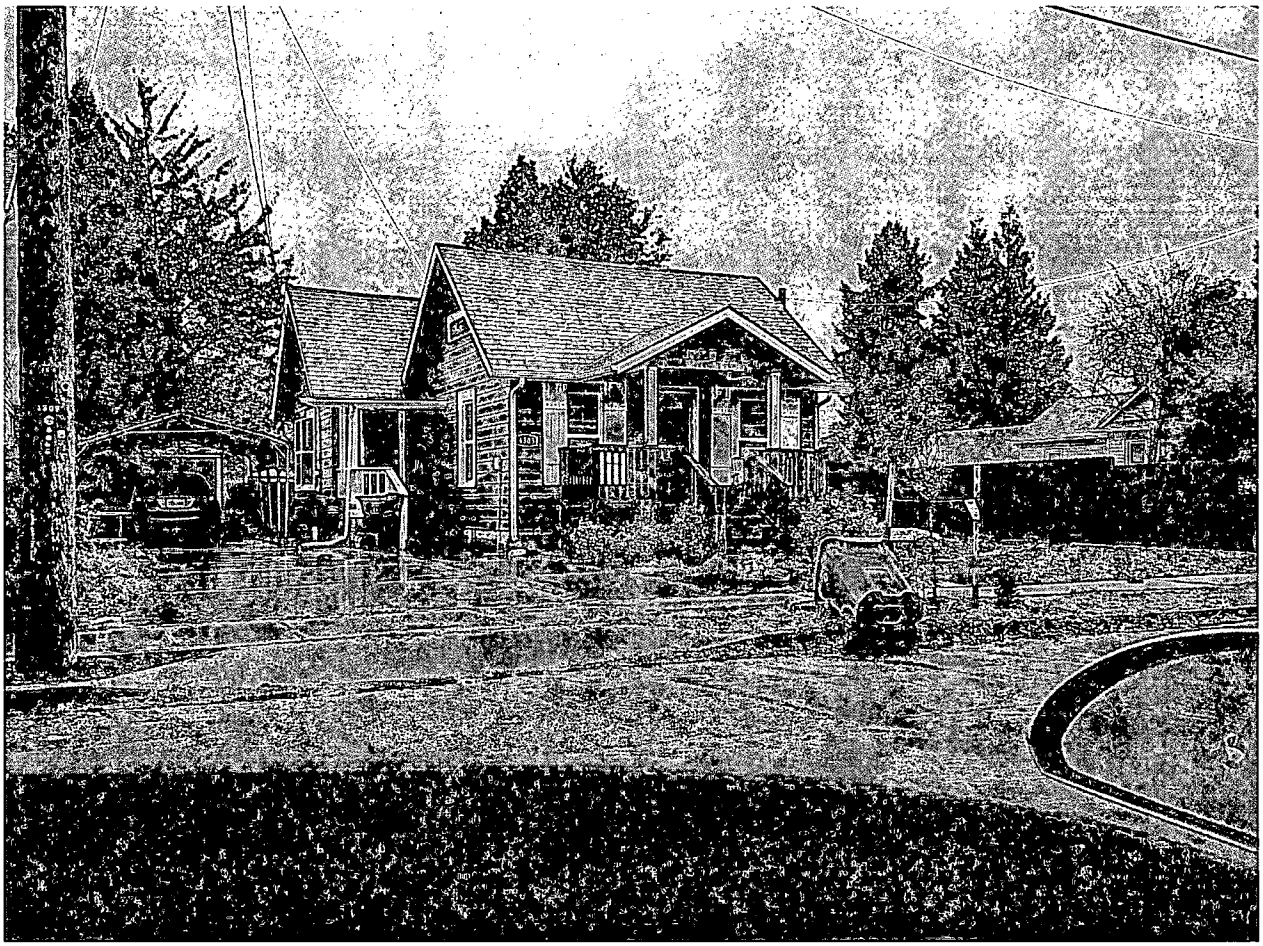
ATTACHMENT A

ATTACHMENT A

1. DESCRIPTION OF PREMISES TO BE SEARCHED

The residence located at 4303 SE 76th Avenue, Portland, Oregon 97206 is identified as a detached, blue, single family home with white shutters and a brown, wooden front porch, depicted below. The house number, 4303, is displayed on the front of the home. There is a driveway on the left side of the residence that leads to a side entrance to the residence, and to a detached carport with what appears to be a shed or storage unit directly behind the carport.

The premise to be searched includes any structures to the real property that is the SUBJECT PREMISES of 4303 SE 76th Avenue, Portland, Oregon 97206, and any storage units or outbuildings, including the carport and shed or storage unit directly behind the carport.



ATTACHMENT A (CONTINUED)

2. DESCRIPTION OF PERSON TO BE SEARCHED

JUAN CARLOS RAMON (a/k/a Carlos Ramon and Juan Ramon) (Provided Found in Oregon)

DOB: 2/10/85

RESIDENCE: 4303 SE 76th Avenue, Portland, OR

Physical Description from last known Driver's License (CA, photo taken in 2008):

Eyes: Brown

Hair: Black

Height: reported 5'9"

Weight: reported 160 lbs

2008 PHOTO:

ATTACHMENT B

ATTACHMENT B

Items to Be Seized

The items to be searched for, seized, and examined, are those items on the premises/person referenced in Attachment A, that constitute or contain evidence, contraband, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2251(a) and (e) (Production and Attempted Production of Child Pornography); 2252A(a)(1) and (b)(1) (Transportation and Attempted Transportation of Child Pornography); 2252A(a)(2)(A) and (b)(1) (Receipt, Distribution, and Attempted Receipt and Distribution of Child Pornography); 2252A(a)(5)(B) and (b)(2) (Knowing Possession or Access and Attempted Access With Intent to View Child Pornography); and 2252A(a)(6) (Sending or Providing a Minor a Visual Depiction That Is, or Appears to Be, a Minor Engaging in Sexually Explicit Conduct, For the Purpose of Inducing or Persuading a Minor to Participate in Illegal Activity).

1. The items referenced above to be searched for, seized, and examined are as follows:

a. All visual depictions of minors engaged in sexually explicit conduct, as defined in 18 USC 2256, including all motion pictures or digital video clips containing such visual depictions;

b. All video recordings which are self-produced and pertain to sexually explicit images of minors, or video recordings of minors which may assist in the location of minor victims of child exploitation or child abuse;

c. All records and information, including written or electronic correspondence or communications, pertaining to the production, transportation, shipment,

distribution, receipt, trade, sale, purchase, or possession of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 USC 2256, or any attempt to commit any such offense, and any attempts to access with intent to view any such depictions;

d. All records or information that pertain to offers to transmit, the solicitation of a transmission, or the transmission, through interstate or foreign commerce by any means (including by computer), of any visual depiction of a minor engaged in sexually explicit conduct, as defined in 18 USC 2256;

e. All records or information naming or identifying minors visually depicted while engaging in sexually explicit conduct, as defined in 18 USC 2256;

f. All records or information pertaining to the user account name @lexithetiger, including any records or information revealing the identity of the person(s) using that account name;

g. Any records of Internet usage, including records containing screen names, user names, and e-mail addresses, and identities assumed for the purposes of communication on the Internet. These records include billing and subscriber records, chat room logs, e-mail messages, and include electronic files in a computer and on other data storage media, including CDs or DVDs;

h. All records or information referring or pertaining to communications with others, whether in person, by telephone, or online, for the purpose of producing, distributing, transporting, receiving, possessing, or viewing child pornography as defined in 18 USC 2256, including chat logs, call logs, address books or contact list entries, digital images sent or received, and the like;

i. All records or information pertaining to the use of Musical.ly and Golden Frog GmbH;

j. All images and video clips of child erotica, defined as material or items that may be sexually arousing to persons having a sexual interest in children but that are not in and of themselves legally obscene and do not depict minors engaged in sexually explicit conduct as defined in 18 USC 2256, such as images of minors depicted in underwear or partially undressed;

k. Computers, storage media, or digital devices used as a means to commit or facilitate the violations described above; and

l. A Visa credit card with the number 481583XXXXXX0193.

2. As used in this attachment, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form. The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware. The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

3. For any computer or storage medium whose seizure is otherwise authorized by this warrant and any computer, storage medium, or digital device that contains or in which is

stored records or information that is otherwise called for by this warrant (hereinafter "Computer"):

a. Evidence of who used, owned, or controlled the Computer at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence.

b. Evidence of software that would allow others to control the Computer, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software.

c. Evidence of the lack of such malicious software.

d. Evidence indicating how and when the Computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crimes under investigation and to the Computer user.

e. Evidence indicating the Computer user's state of mind as it relates to the crimes under investigation.

f. Evidence of the attachment to the Computer of other storage devices or similar containers for electronic evidence.

g. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Computer.

h. Evidence of the times the Computer was used.

i. Passwords, encryption keys, and other access devices that may be

necessary to access the Computer.

j. Documentation and manuals that may be necessary to access the Computer or to conduct a forensic examination of the Computer.

k. Records of or information about Internet Protocol addresses used by the Computer.

l. Records of or information about the Computer's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

m. Contextual information necessary to understand the evidence described in this attachment.

n. Routers, modems, and network equipment used to connect computers to the Internet.

4. During the execution of the search of the Premises/Person described in Attachment A, law enforcement personnel are authorized to press the fingers, including thumbs, of **JUAN CARLOS RAMOS, a/k/a Carlos Ramos and Juan Ramos,** found at the Premises to the Touch ID sensor of the Apple brand device(s), such as an iPhone or iPad, found at the Premises for the purpose of attempting to unlock the device(s) via Touch ID in order to search the contents as authorized by this warrant.

Search Procedure

5. The search for data capable of being read, stored, or interpreted by a computer or storage device, may require authorities to employ techniques, including imaging any computer or

storage media and computer-assisted scans and searches of the computers and storage media, that might expose many parts of the computer to human inspection in order to determine whether it constitutes evidence as described by the warrant.

6. The initial examination of the computer and storage media will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

7. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the computer and storage media do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

8. If an examination is conducted, and the computer and storage media do not contain any data falling within the ambit of the warrant, the government will return the computer and storage media to its owner within a reasonable period of time following the search and will seal any image of the computer and storage media, absent further authorization from the Court.

9. The government may retain the computer and storage media as evidence, fruits,

contraband, or an instrumentality of a crime or to commence forfeiture proceedings against the computer and storage media and/or the data contained therein.

10. The government will retain a forensic image of the computer and storage media for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.